LISBON
SCHOOL OF
ECONOMICS &
MANAGEMENT
UNIVERSIDADE DE LISBOA

MESTRADO
GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO
PROJECTO

LEVANTAMENTO DE REQUISITOS E DESENVOLVIMENTO DE FERRAMENTA DE REGISTO DE INCIDENTES DE RISCO

Nuno Miguel Monteiro dos Santos

LISBON SCHOOL OF ECONOMICS & MANAGEMENT
UNIVERSIDADE DE LISBOA

MESTRADO
GESTÃO DE SISTEMAS DE INFORMAÇÃO

TRABALHO FINAL DE MESTRADO
PROJECTO

LEVANTAMENTO DE REQUISITOS E DESENVOLVIMENTO DE FERRAMENTA DE REGISTO DE INCIDENTES DE RISCO

Nuno Miguel Monteiro dos Santos

ORIENTAÇÃO:

Doutor Carlos J. Costa, Professor Associado

Índice

Índice de Figuras

Lista de Tabelas

Agradecimentos

O espaço limitado desta secção de agradecimentos, seguramente, não me permite agradecer, como devia, a todas as pessoas que, ao longo do meu Mestrado em Gestão de Sistemas de Informação me ajudaram, direta ou indiretamente, a cumprir os meus objetivos e a realizar mais esta etapa da minha formação académica. Desta forma, deixo apenas algumas palavras, poucas, mas um sentido e profundo sentimento de reconhecido agradecimento.

Ao Coordenador do Mestrado em Gestão de Sistemas de Informação, Professor Doutor António Palma dos Reis, agradeço a oportunidade e o privilégio que tive em frequentar este Mestrado que muito contribuiu para o enriquecimento da minha formação académica e científica.

Ao professor Carlos Costa especialmente por ter aceitado a orientação do meu Trabalho Final de Mestrado, que espero conseguir retribuir a confiança depositada.

Aos professores da Pós-Graduação STIO, que direta e indiretamente contribuíram partilhando os seus conhecimentos e experiencias que foram sem dúvidas, importantes para o meu crescimento académico.

Aos colegas de curso por todas sugestões e partilhas de conhecimentos e pela solidariedade e amizade demostrada ao longo desta nossa etapa final do curso.

Acrónimos, Abreviaturas, Siglas e Convenções

BCBS	*Basel Committee on Banking Supervision*
BD	*Base de Dados*
BIS	*Bank for International Settlements*
BNA	*Banco Nacional de Angola*
CA SDM	*CA Service Desk Manage*
CobiT	*Control Objectives for Information and related Technology*
DRI	*Departamento de Risco*
DTI	*Departamento de Tecnologias de Informação*
GRO	*Gestão de Risco Operacional*
ISO	*International Organization for Standardization*
IT	*Information Technology*
ITIL	*Information Technology Infrastructure Library*
LDAP	*Lightweight Directory Access Protocol*
OGC	*UK Office of Government Commerce*
SDM	*Service Desk Manager*
SI	*Sistemas de Informação*
SLA	*Service Level Agreement*
PDCA	*Plan, Do, Check, Action*
RO	*Risco Operacional*
UE	*Unidade de Estrutura*

Resumo

O presente trabalho de mestrado visa otimizar o processo de gestão de risco, bem como alinhar a instituição em conformidade com as normas e boas práticas internacionais de gestão do risco operacional. Desenvolveu-se uma solução que integra a classificação e registo dos riscos associados a todos incidentes registados no Banco Nacional de Angola (BNA). Iniciou-se o projeto com a análise e levantamento de requisitos, onde foi feita uma análise detalhada dos requisitos definidos pelo cliente, o departamento de Gestão de risco (DRI). Com isso foi possível atingir o objetivo, criando um sistema de informação, bem como um processo que permita deter e analisar a informação dos principais riscos a que o Banco está exposto. Este sistema não só responde a uma necessidade clara do DRI, em gerir os incidentes e os riscos associados, como fornece uma *framework* de gestão de risco alinhado com as normas e melhores praticas definidas pelas instituições internacionais no âmbito da gestão de incidentes. A implementação desta ferramenta vai gerar uma mudança significativa no processo organizacional do BNA, nomeadamente em questões politicas, culturais e humanas.

Palavras-chave: Gestão de Risco, Gestão de Risco Operacional; Normas e Melhores Práticas, Sistema de Informação, Processo organizacional.

Abstract

This master project research intends to optimize the risk management process, as well as to align the institution in accordance with the international standards and good practices of operational risk management, a solution was developed that integrated the classification and recording of the risks associated with all incidents registered with the National Bank of Angola (BNA). The project began with the analysis and survey of requirements, where a detailed analysis of the requirements defined by the client, the DRI department, was made. With this, it was possible to achieve the objective by creating an information system, as well as a process that allows collect and analyze the information of the main risks to which the Bank is exposed. This system not only responds to a clear need for the department of risk management (DRI), to manage incidents and associated risks, but also provides a risk management framework in line with the standards and best practices defined by international institutions in incident management. The implementation of this tool will generate a significant change in the organizational process of the BNA, namely in political, cultural and human issues.

Keywords: Risk Management, Operational Risk Management; Standards and Best Practices, Information System, Organizational Process.

1. INTRODUÇÃO

Os Sistemas de Informação servem para otimizar os fluxos de informação e de conhecimento dentro (e dentre) as organizações. O sistema de informação é todo o processo administrativo que utiliza da tecnologia da informação, de pessoas e estruturas dentro de uma organização, transformando em processos de menor dimensão para gerar armazenamento, processamento e saída de informações. Assim fazem com que os dados fluam sem descontinuidade por todos os setores da organização como também entre os parceiros da mesma. (Martins *et al.*, 2012)

A Tecnologia da Informação vai muito mais além do que possuir equipamentos de tecnologia avançada, ou seja, trata-se de uma ação que envolve estratégia em que vários fatores devem ser levados em consideração para que a implantação da mesma propicie os melhores resultados para o processo decisório. A tecnologia da informação precisa ser aplicada de forma planeada, utilizando os procedimentos adequados para que não corra um risco elevado e imensurável. O ambiente da organização deve estar preparado para receber essa tecnologia e fazer uso dela. (Martins *et al.*, 2012)

A década de 1990 foi marcada pelo reforço do processo de inovação financeira, motivado, em especial, pelo desenvolvimento e integração dos mercados financeiros, pela evolução tecnológica no domínio dos sistemas de informação e pelos avanços científicos na área da economia financeira. Em consequência, o sector bancário tem vindo a adotar técnicas progressivamente mais sofisticadas de avaliação dos riscos, em especial nas vertentes do risco de crédito, dos riscos de mercado e do risco operacional. (Decreto-Lei n.º 104/2007 de 3 de abril)

Desde a revisão do Acordo de Basileia tem sido requerido das instituições financeiras que se mantenha capital suficiente para cobrir perdas financeiras provenientes de eventos de risco operacional. Assim, segundo o Basel Committee on Banking Supervision (2006) a quantificação do risco operacional passou a receber crescente atenção, tanto por parte das instituições financeiras quanto pelos decisores políticos. A estes caberão, em última instância, a tarefa de avaliar, julgar e anuir (ou não) para com as estratégias de gerenciamento, de administração e de controlo do risco, bem como quanto à metodologia de cálculo dos riscos, dos instrumentos de mitigação e cobertura de risco utilizados.

1.1. Problema

O Banco Nacional de Angola, abreviadamente designado por BNA, fundado em 5 de Novembro de 1976, é uma pessoa coletiva de direito público, dotada de autonomia administrativa, financeira e patrimonial.

O Banco Nacional de Angola, como banco central e emissor de moeda, assegura a preservação do valor da moeda nacional e participa na definição das políticas monetária, financeira e cambial.

No Departamento de Risco (DRI) do Banco Nacional de Angola (BNA), tem como uma das suas atribuições assegurar a gestão integrada dos riscos associados à atividade do Banco, com base na identificação, avaliação, monitorização e controlo de todos os riscos que possam influenciar a estratégia e os objetivos definidos.

Com base no acordo de Basileia II, e as normas ISO 31000, torna-se necessário implementar mecanismos de registo e gestão de incidentes (com eventos de risco), como parte integrante da Gestão de Risco Operacional.

1.2. Objetivos

O presente Projeto tem como objetivo o desenvolvimento de uma solução suportada informaticamente para otimização dos processos do Departamento de Risco (DRI) no que se refere ao registo de incidentes e eventos de risco, como parte integrante da Gestão de Risco Operacional (GRO), de modo deter a informação dos principais riscos a que o Banco está exposto.

2. REVISÃO DE LITERATURA

2.1. Tecnologia e Sistemas de Informação

Os Sistemas de Informação podem ser entendidos como processos administrativos que envolvem processos menores que interagem entre si, integrando-se para armazenarem dados e gerar informações para contribuir nas decisões. Os Sistemas de Informação são criados aproveitando os conceitos da Tecnologia da Informação e fornecem condições para que as instituições possam tomar decisões corretas e exatas, propiciando que a mesma venha sempre a atingir um melhor desempenho. (Martins *et al.*, 2012)

Segundo Spinola e Pessôa (1998, p.98), um "Sistema de Informação (S.I.) é um sistema que cria um ambiente integrado e consistente, capaz de fornecer as informações necessárias a todos os usuários" ou ainda, como (Schutzer & Pereira, 1999, p.149) "é um sistema integrado homem-máquina que fornece informações de suporte a operações, gerenciamento, análise e funções de tomada de decisões em uma organização".

Em relação à segunda abordagem, (Ribeiro & Vieira, 2001) define Sistema de Informação como uma rede baseada em computador, contendo sistemas operacionais que fornecem à administração dados relevantes para fins de tomada de decisões.

Um sistema de Informação é um conjunto de meios humanos e técnicos, dados e procedimentos que se articulam entre si, tendo em vista atingir um objetivo comum: fornecer informação útil para o desenvolvimento das atividades da organização em que está inserida, e que podem ir desde atividades operacionais até à definição dos objetivos estratégicos e ao processo de tomada de decisão (Ventura, 1992).

A definição de sistemas de informação de acordo com O'Brien (2004, p.6) "é um conjunto organizado de pessoas, *hardware*, *software*, redes de comunicações e recursos de dados que coleta, transforma e dissemina informações em uma organização. Para que uma organização possa disseminar as informações, depende basicamente destes recursos". Para (Laudon & Laudon, 2013), um sistema de informação pode ser definido tecnicamente como um conjunto de componentes inter-relacionados que coletam (ou recuperam), processam, armazenam e distribuem informações para apoiar a tomada de decisões e o controle em uma organização. Além de apoiar a tomada de decisões, a coordenação e o controle, os sistemas de informação também podem ajudar os gestores e os colaboradores a analisar problemas, visualizar assuntos complexos e criar novos produtos.

Os sistemas de informação contêm informações sobre pessoas, lugares e coisas importantes na organização ou no ambiente que o rodeia. Por informação, queremos dizer dados que foram moldados em uma forma que é significativa e útil para os seres humanos. Os dados, em contraste, são fluxos de fatos brutos que representam eventos que ocorrem em organizações ou o ambiente físico antes de terem sido organizados e organizados em uma forma que as pessoas possam

compreender e usar. (Laudon & Laudon, 2013).

2.2. ITIL

ITIL é a abreviação para *Information Technology Infrastructure Library*, é uma estrutura pública que descreve boas práticas para gerenciamento de serviços de TI e se concentra

no alinhamento de serviços de TI com as necessidades de negócios, medição contínua e melhoria da qualidade do serviço de TI entregue ao negócio e ao cliente. (Cartlidge *et al.*, 2007).

As práticas de ITIL são aplicadas nas múltiplas modalidades da prestação de serviços de TI, com elevada enfase nos aspetos tecnológicos e na integração de requisitos de negócio. Este referencial tem sido utilizado em projetos de teor infraestrutural, como o suporte a aplicações, suporte a utilizadores, manutenção de equipamentos, entre outros. (Fernandes & Abreu, 2014)

Segundo (Cartlidge *et al.*, 2007), para se ter uma definição de o que é ITIL® é importante entender que ela é organizada em torno do ciclo de vida de um serviço dentro de uma organização e contém os seguintes volumes:

- Estratégia do Serviço ("*Service Strategy*"): Definição dos requisitos e necessidades do negócio;
- Projeto de Serviço ("*Service Design*"): Definição da solução a ser adotada;
- Transição de Serviço ("*Service Transition*"): Relacionado ao gerenciamento de mudanças;
- Operação do Serviço ("*Service Operation*"): Assegura que os serviços estão sendo atendidos baseado nos *SLAs*;
- Melhoria Contínua do Serviço ("*Continual Service Improvement*"): Manter a constante melhoria dos serviços baseando-se no ciclo PDCA[1].

1 PDCA - O ciclo PDCA foi criado na década de 20 por Walter Andrew Shewart, um físico norte-americano conhecido por ser pioneiro no controle estatístico de qualidade. Significa Plan, Do, Check, Action

Figura 1 - Ciclo de Vida ITIL

Fonte: itSMF (2007)

Dentre os principais benefícios do uso do modelo ITIL V3 podemos mencionar (Cartlidge *et al.*, 2007):

- Alinhamento de TI, seus serviços e riscos com as necessidades do negócio
- Níveis de Serviço (SLA) negociáveis
- Processos consistentes e previsíveis
- Eficiência na entrega de serviço
- Serviços e Processos mensuráveis e passíveis de melhorias
- Otimização da experiência do cliente
- Uma linguagem comum

2.2.1. Gestão de Incidentes vista pelo ITIL

Um Incidente é qualquer evento que não faz parte do funcionamento *standard* de um serviço e que provoca ou pode provocar uma interrupção no serviço ou uma redução na respetiva qualidade. (Macfarlane & Rudd, 2005)

Segundo a *framework* ITIL v3 (Cartlidge *et al.*, 2007), repor o normal funcionamento do serviço tão rapidamente possível com o mínimo de interrupção do negócio, assegurando assim que os melhores níveis de disponibilidade e serviço pretendido são mantidos.

A Gestão de Incidentes para (Cartlidge *et al.*, 2007) permite:

- Assegurar a melhor utilização de recursos para apoiar o negócio;
- Desenvolver e manter registos significativos relativamente aos Incidentes;
- Definir e aplicar uma abordagem consistente a todos os Incidentes comunicados.

Exemplos de Incidentes:

- Aplicação indisponível aos clientes;
- Avaria ou limitação na utilização do equipamento;
- Bloqueio contínuo da aplicação de negócio;
- Falha nas comunicações de dados.

Responsabilidades da Gestão de Incidentes:

- Deteção e registo de Incidentes;
- Classificação de todos os Incidentes e apoio inicial;
- Investigação e diagnóstico;
- Resolução e recuperação;

- Eliminação do Incidente;
- Propriedade, controlo, rastreio e comunicação do Incidente.

Fatores de sucesso fundamentais na Gestão de Incidentes:

- Existência de uma base de dados de Gestão de Configurações (CMDB) atualizada;
- Existência de uma base de conhecimento com o registo dos dados dos problemas e dos erros conhecidos, resoluções e soluções;
- Disponibilização de ferramentas eficazes e automatizadas;
- Relacionamento estreito e efetivo com a Gestão de Níveis de Serviço.

2.3. Gestão de Risco Operacional

Antes de se falar em GRO, é preciso entender o que é o Risco. Segundo a ISO[2] (2009) define os riscos como o efeito da incerteza sobre os objetivos. Nesta definição, a incerteza inclui eventos (que podem ou não acontecer) e as incertezas causadas pela ambiguidade ou falta de informação (Nelson & Katzenstein, 2008). Também inclui impactos negativos e positivos nos objetivos (ISO, 2009).

Para dar um conceito a Risco Operacional devemos recorrer a diversas definições e por norma geral o se considera risco operacional, o tipo de risco que, ao contrário do podemos crer, não é o mesmo que risco de mercado ou risco de crédito. Se vamos a outros conceitos as definições incluem uma nova categoria de risco diferente: o risco chamado risco legal.

[2] ISO: International Organization for Standardization

A definição de Risco Operacional faz explícita referência a perdas que são derivadas de processos inadequados ou falhas de índole interna, provocadas por erro humano ou até mesmo de sistema. Também podemos dizer que risco operacional é aquele decorrente de fatores externos, de acordo com o (Basel Committee on Banking Supervision, 2006).

Ao fazer uma retrospetiva histórica, é possível observar que os riscos financeiros, de um modo geral, sempre tiveram maior importância que os riscos operacionais. No entanto, Tschoegl (2005) menciona que as experiências dos últimos anos têm sugerido que o risco operacional foi responsável por muitos dos grandes desastres ocorridos, principalmente em instituições financeiras.

Esses desastres e crises foram mais evidentes na década de 90, com escândalos internacionais ocorridos em empresas de renome (como Bankers Trust - 1994, Credit Lyonnais - 1994, Barings - 1995, Daiwa Bank - 1995, Nacional - 1995, Sumitomo - 1996, para citar alguns), o que levou os órgãos reguladores à conclusão de que não era suficiente para a indústria financeira gerir corretamente apenas os riscos de crédito e mercado, havia também a necessidade de manter sob controlo os riscos operacionais. (Jorion, 2006, Pedrosa & Costa, 2012)

O risco operacional tornou-se um dos temas mais discutidos por académicos e profissionais do setor financeiro nos últimos anos. Os motivos dessa atenção podem ser atribuídos a maiores investimentos em sistemas de informação e tecnologia, a crescente onda de fusões e aquisições, o surgimento de novos instrumentos financeiros e o crescimento da negociação eletrônica (Sironi & Resti, 2007). Além disso, o Novo Acordo de Capital de Basileia (efetivo desde 2007) exige um requisito de capital para o risco

operacional e motiva ainda mais as instituições financeiras a medir e gerenciar mais precisamente esse tipo de risco.

Na definição de (Duarte, 1999), risco operacional é uma medida das possíveis perdas em uma instituição, no caso de seus sistemas, práticas e medidas de controlo não serem capazes de resistir às falhas humanas ou a situações adversas de mercado. Para (Cruz, 2002) refere-se a perdas originadas de erros operacionais de qualquer espécie que afetem o lucro dos bancos. Segundo a definição adotada pelo BIS[3], o conceito de risco operacional está relacionado aos riscos de perdas decorrentes de falhas ou inadequações de pessoas, processos, sistemas ou de eventos externos; incluindo riscos legais e excluindo riscos estratégicos e de imagem (*strategic and reputational risk*).[4]

No setor bancário, o Risco Operacional é definido como os riscos do banco além dos riscos de crédito e de mercado. Em geral, refere-se aos riscos dos bancos causados por processos internos ineficientes, implementação incorreta de pessoal e fatores externos (Basel Committee on Banking Supervision, 2011). Como pode ser entendido a partir desta definição, o risco operacional é o risco mais comum que é encontrado no processo comercial diário. O risco operacional contém principalmente quatro aspetos diferentes, que são pessoas, sistemas, processos e fatores externo (van den Brink, 2002).

Existem muitas definições de risco operacional, como o risco decorrente de erros e acidentes humanos e técnicos (Jorion, 2000) ou uma medida do vínculo entre as atividades comerciais da empresa e a variação nos resultados comerciais (King, 2001).

[3] Bank International of settlement

[4] *Basel II: International Convergence of Capital Measurement and Capital Standards: a Revised Framework - Comprehensive Version – Junho de 2006.*

O Comitê de Basileia oferece uma definição mais precisa de risco operacional como "o risco de resultar de processos internos, pessoas e sistemas inadequados ou falidos ou de falhas de eventos externos" (Basel Committee on Banking Supervision, 2006, p.144). Esta definição abrange uma área de risco relativamente ampla, com a inclusão, por exemplo, de risco estratégico, de transação ou legal (conforme tabela abaixo).

Pessoas	**Sistemas**	**Processos**	**Fatores externos**
Fraude, colusão e outras atividades criminosas	Problemas de TI (falhas de hardware ou software, *hacking* de computador ou vírus)	Erros de execução, registro, liquidação e documentação (risco de transação)	Atividades criminosas (roubo, terrorismo ou vandalismo)
Violação de regras internas ou externas (negociação não autorizada, abuso de informações)	Acesso não autorizado a informações e sistemas de segurança	Erros em modelos, metodologias e *market-to-market* (modelo de risco)	Eventos políticos e militares (guerras e sanções internacionais)
Erros relacionados à incompetência ou negligência de gerenciamento	Indisponibilidade falta de integridade de dados	Erros de contabilidade e de tributação. Implantação inadequada dos procedimentos internos.	Mudança no ambiente político, regulamentar e fiscal (risco estratégico)
Perda de funcionários importantes (doença, lesão, problemas na retenção de pessoal)	Falha de telecomunicações	Questões de conformidade. Violação do mandato	Mudança no ambiente legal (risco legal). Eventos naturais (fogo, terremoto, inundação)
Violações da segurança de sistemas	Redução na utilização	Definição inadequada e atribuição de responsabilidades	Falha operacional em fornecedores ou operações terceirizadas

Tabela 1 - Risco Operacional

Fonte**:** Sironi & Resti (2007)

De um modo geral, quando se trata de gerir o risco, devem distinguir-se duas posições: uma primeira visão proactiva, baseada na identificação e controle de fatores de risco, embora ainda não se tenham materializado em perdas; e, por outro lado, a postura reativa, que serve para executar o plano de contingência assim que o evento ocorreu. A estratégia proactiva permite minimizar possíveis impactos negativos através do fortalecimento dos controles operacionais. Em qualquer caso, independentemente da abordagem adotada, a gestão do risco operacional deve ser alinhada com três objetivos fundamentais para uma instituição financeira:

1. Assegurar a continuidade do negócio a longo prazo da entidade.
2. Estimular a melhoria contínua dos processos e aumentar a qualidade do serviço ao cliente.
3. Cumprir o quadro regulamentar estabelecido e otimizar a alocação de capital.

A este respeito, o (Basel Committee on Banking Supervision, 2003), no seu documento " Sound Practices for the Management and Supervision of Operational Risk", contém um compêndio de princípios sobre tendências e práticas atuais na gestão e supervisão do risco operacional que, devem ser levados em consideração pelos bancos e pelas autoridades de supervisão. Enquanto o (Basel Committee on Banking Supervision, 2011) atualizou este documento, a versão revisada destaca a evolução da gestão de riscos operacionais desde 2003. Os princípios delineados no relatório examinam três aspetos principais: estrutura de governança, gestão de riscos e divulgação de informações. As

diretrizes de gerenciamento implícitas no documento são ilustradas sinopticamente na figura abaixo:

Figura 2 - Princípios de Gestão de Risco Operacional

Fonte: BCBS (2014a, 2014, 2011) e Jiménez (2013)

2.4. Engenharia de Requisitos

O sucesso no desenvolvimento de um *software* é mensurado principalmente pela forma com que ele executa a tarefa para qual foi proposto (Nuseibeh & Easterbrook, 2000). O esforço de desenvolvimento é total ou parcialmente desperdiçado se o *software*, por melhor que seja a qualidade de sua codificação, não cumpre com a tarefa a que foi destinado. Da mesma forma, se a base tecnológica (*hardware*, *software*) necessária ao *software* em questão não for compatível com a base existente onde ele será utilizado, todo (ou a maior parte) o trabalho de desenvolvimento pode se tornar inútil. Para que o sucesso possa ser atingido, é essencial que seja efetuada uma tarefa de identificação e documentação das necessidades e propósitos de um *software*. Esta tarefa, muitas

vezes, exige uma compreensão do ambiente onde o *software* será inserido, considerando as características do negócio, as possíveis modificações futuras e as necessidades reais envolvidas no processo.

Segundo (Pressman, 2001) não existe uma forma incontestável de garantir que a especificação de um sistema está propriamente de acordo com as necessidades do cliente, e que satisfaz suas necessidades. Este é um desafio complexo enfrentado pelos engenheiros de *software*, e o melhor modo de encará-lo é através de um processo consistente de engenharia de requisitos.

No presente capítulo pretende-se apresentar conceitos primários e é destacada a relevância da engenharia de requisitos no processo de desenvolvimento de *software*, de acordo com a visão de diversas bibliografias.

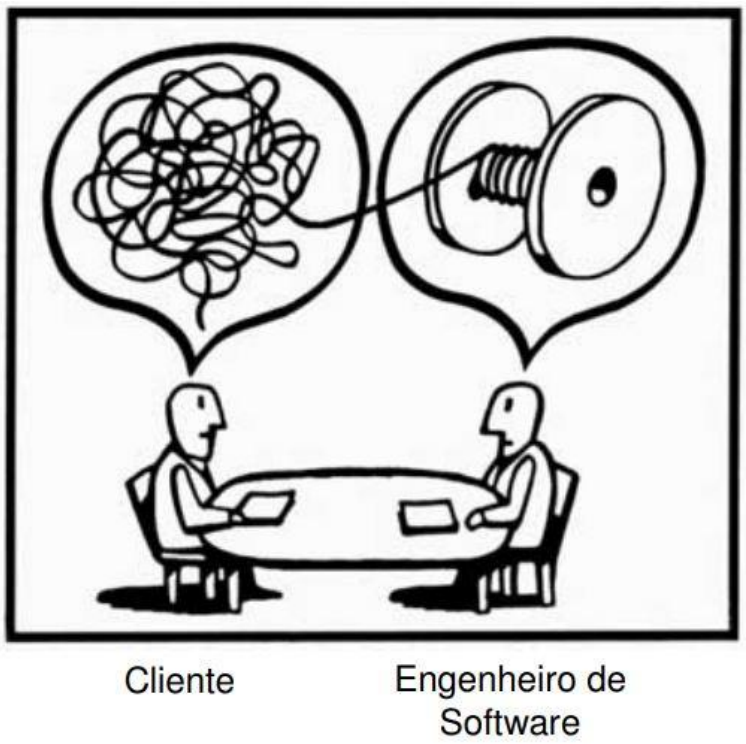


Figura 3 – Comunicação

Fonte: tinybuddha

(Pressman, 1995) utilizava o termo análise de requisitos, para referir-se ao processo como um todo. Mais a frente, (Pressman, 2001), adotou o termo engenharia de requisitos, considerando a análise de requisitos como uma de suas etapas.

(Sommerville, 2007), tem como objetivo definir o que o sistema deve fazer, quais as necessidades reais e identificar quais restrições existem para que o *software* seja desenvolvido. É nesse processo da engenharia de *software* que ocorre a comunicação entre o cliente e o analista da equipe de desenvolvimento. Quando essa comunicação não é bem-sucedida, o restante do projeto pode ficar comprometido, causando impacto no custo e prazo.

Software deve ser entendido como uma ferramenta de suporte à solução de problemas com o uso da informática (Zanlorenci, 1999).

(Siddiqi, 1996) define requisitos como uma declaração completa do que o *software* irá fazer sem referir-se a como fazê-lo. (Kruchten, 2000) define um requisito como uma condição ou capacidade que um *software* deve realizar.

(Gougen, 1996) acrescenta mais um elemento a esta definição, que se tem mostrado importante na utilização de requisitos. Em sua visão, requisitos são propriedades que um *software* deve possuir para funcionar com sucesso no ambiente onde será utilizado.

Diversos autores dividem os requisitos em dois tipos: funcionais e não funcionais.

De acordo com (Kruchten, 2000), requisitos funcionais são utilizados para expressar o comportamento de um *software* através da especificação das condições de entrada e saída que deve possuir. Requisitos não-funcionais são atributos desejados de qualidade que não são descritos pelos requisitos funcionais.

Segundo (Zave, 1997), a engenharia de requisitos é a área da engenharia de *software* que se preocupa com as metas reais, funções e restrições de software. Ela também se preocupa com o relacionamento destes fatores com uma precisa especificação do comportamento do *software* e sua evolução através do tempo e das famílias de software.

Sommerville, (2007) define que o processo de engenharia de requisitos é composto de quatro atividades: estudo de viabilidade, levantamento e análise de requisitos, documentação dos requisitos e, por fim, validação dos requisitos. Ao final dessas atividades, é obtido o documento de requisitos.

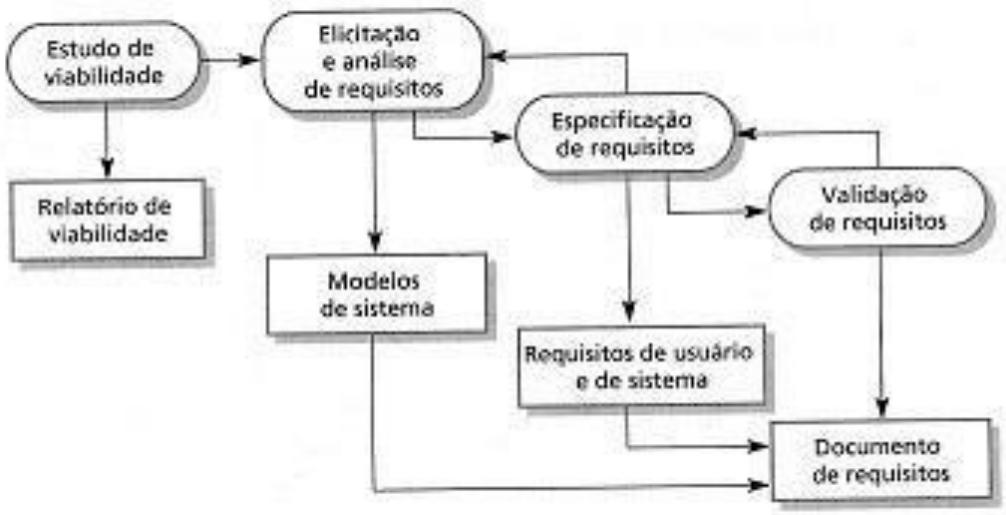


Figura 4 - Processo de Engenharia de Software

Fonte: Sommerville (2007)

A atividade de estudo de viabilidade é o primeiro passo para o desenvolvimento do *software*. É nesse momento que ocorre uma primeira comunicação entre o cliente e o analista da equipe de desenvolvimento. Segundo Sommerville (2007), os resultados

dessa atividade definem se o sistema a ser construído contribui ou não para a organização.

Sommerville (2007) afirma que para se obter as informações do escopo do projeto, é necessário que possíveis perguntas sejam respondidas pelo cliente, por exemplo:

- Como a organização se comportaria se esse sistema não fosse implementado?
- Quais são os problemas com os processos atuais e como o novo sistema ajudaria a reduzir esses problemas?
- Qual será a contribuição direta do sistema para os objetivos e requisitos da empresa? 4. As informações podem ser transferidas e recebidas de outros sistemas da organização?
- O sistema requer tecnologia que ainda não foi usada na organização?

Com as respostas destas questões, o analista terá a capacidade de determinar qual a importância do sistema para a organização, expondo seu funcionamento para o cliente, de modo que no final o produto solicitado otimize os processos da empresa.

Levantamento e Analise de Requisitos realiza o levantamento das necessidades do usuário, isto é, os requisitos do sistema, por meio de diversas técnicas.

Para Sommerville (2007), a atividade de análise de requisitos visa priorizar e resolver conflitos entre requisitos, pois quando vários usuários participam desse processo, é inevitável que ocorra contradição entre requisitos levantados de usuários distintos. Nesta atividade, o analista inicia uma comunicação com o cliente utilizando técnicas para que possa obter o conhecimento das necessidades do usuário. Com as respostas obtidas, é possível identificar quais serviços o sistema deve oferecer, quais as suas

restrições, o que é esperado pelo cliente e demais informações, tal como a possibilidade de integração com outros sistemas.

A especificação de requisitos é escrita pelo analista, contendo as informações que foram recolhidas no levantamento dos requisitos. Para Pressman, (2010), a especificação é o documento de trabalho que servirá como referência para as demais atividades da engenharia de *software*. O documento contém informações sobre o que o sistema deve fazer, quais as necessidades reais e quais restrições existem para que o *software* seja desenvolvido.

Para Sommerville (2007), a validação de requisitos tem como objetivo garantir que a necessidade real do cliente esteja descrita corretamente no documento de especificação dos requisitos. A validação é extremamente importante, pois o custo para correção de um requisito nessa fase é bem inferior ao custo nas fases posteriores, como implementação ou testes. Isso ocorre, pois, se defeitos encontrados nessas fases, os requisitos devem ser novamente levantados e posteriormente são implementados e testados.

Pressman, (2010) afirma que os requisitos devem ser examinados para que sejam encontradas inconsistências, ambiguidades e omissões. Para tal atividade, Sommerville (2007) propõe algumas técnicas de validação, tais como revisões de requisitos, prototipagem e geração de casos de teste.

2.5. Síntese da Revisão de Literatura

As tecnologias de informação estão na origem de mudanças significativas nos modelos de negócio das instituições, com o desenvolvimento e otimização dos SI que dão suporte aos processos e atividades diárias das organizações.

Recorrendo a literatura mencionada acima, conseguiu-se chegar a um entendimento profundo da importância da gestão de incidentes para a gestão de risco operacional. Assim sendo, percebendo-se os pressupostos da GRO, consegue-se mapear um processo de gestão de risco mais eficiente, e baseado nas melhores práticas internacionais como o ITIL, sendo o ele uma importante ferramenta na gestão de incidentes.

A engenharia de requisitos também é uma ferramenta fundamental, porque a tarefa de análise e levantamento de requisitos, muitas vezes, exige uma compreensão do ambiente onde o sistema será inserido, considerando as características do negócio, as possíveis transformações futuras e as necessidades reais envolvidas no processo.

3. ABORDAGEM METODOLOGICA

O presente Projeto tem como objetivo a implementação de uma solução informática para otimização dos processos inerentes à Gestão de Risco Operacional, do Departamento de Risco (DRI), especificamente no que refere à identificação e gestão centralizada e automatizada dos principais eventos de risco a que o Banco está exposto.

Foi utilizada uma abordagem metodológica, que teve como base o processo de desenvolvimento de software conforme bibliografia de Sommerville, a engenharia de requisitos de Pressman, juntamente com o processo interno do BNA, de análise de sistema, utilizado pela equipa de analistas de sistema. Este processo é baseado em atividades da engenharia de requisitos, e consiste nas seguintes fases: Inicio, Análise e Levantamento de Requisitos, Desenvolvimento e Implementação, e Testes.

Como resultado desta metodologia, será implementado um módulo na ferramenta de registo de incidentes de TI, *CA SDM*, para suportar as componentes de registo, análise e reporte dos eventos de risco assim como, possibilitará que todos os intervenientes tenham acesso oportuno e atualizado à informação relevante e possuam uma visão adequada e objetiva das fontes de exposição ao risco.

A ferramenta proposta suportara a componente de registo, análise e reporte do risco operacional.

4. DESCRIÇÃO DO PROJETO

4.1. Inicio

O projeto teve início com a constituição de uma equipa de projeto numa reunião de *kick-off*, e ficaram definidos os intervenientes seguintes:

- Coordenador do projeto – Nuno Santos
- Recursos humanos envolvidos
    - 1 Analista de negócio - DTI
    - 1 Engenheiro de desenvolvimento - DTI
    - 1 Consultor externo - OKWIN
    - 2 Gestores de Risco – DRI

A mesma equipa de projeto fará parte da equipa de testes. O projeto terá uma duração estimada de 3 meses a contar da data de *kick-off*.

Na seguinte reunião, foram definidas as seguintes atividades a desenvolver:

- Análise e levantamento detalhado dos requisitos;
    - Elaborar o documento de Levantamento de Requisitos
    - Elaborar o Project Charter – Analista de Negócio;
- Verificar a possibilidade de ser integrado (desenvolvido) no CA *Service Desk Manager* (Solução que utilizada para *IT Service Desk Manager*)
- Elaborar o documento Termo de Abertura do Projeto (TAP) – Coordenador do Projeto;
- Iniciar o Desenvolvimento após aprovação por parte da Administração do TAP;

- Realização de testes;
- Acompanhamento e formação aos utilizadores;

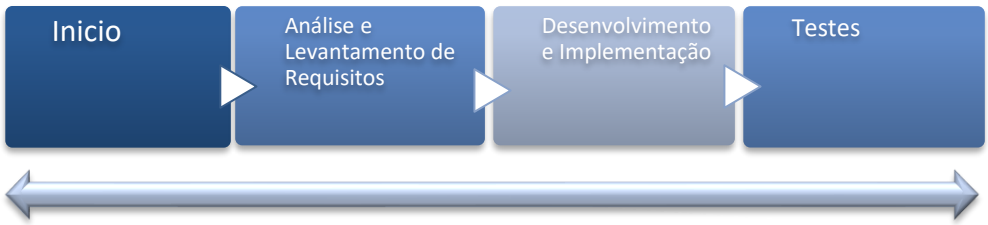


Figura 5- Fases do Projeto

4.2. Análise e Levantamento de Requisitos

O levantamento de requisitos é umas das partes mais importantes do processo que resultará no desenvolvimento de um sistema. Entender aquilo que o cliente deseja ou o que o cliente acredita que precisa e as regras do negócio ou processos do negócio. Isso é o fator determinante que move essa importante função que faz parte da Engenharia de *Software* (Engenharia de requisitos).

Uma das falhas comuns no levantamento de requisitos decorre da ausência de um especialista do negócio ou de alguém que possua experiência nesse ramo do negócio, na equipa do projeto.

Outra das falhas habitualmente citadas é o não mapeamento do processo, que é de vital importância para os resultados obtidos pelo levantamento de requisitos.

Tendo feito parte da equipa do projeto do DTI, uma analista de negócio e de *software*, passamos a realização de reuniões entre DTI e o DRI, onde ficaram definidos os requisitos para o desenvolvimento do projeto.

4.2.1. Caracterização das Necessidades do DRI

Como resultado da reunião para o levantamento de requisitos, dividimos a análise do sistema da seguinte forma:

O registo de incidentes constitui um componente essencial do processo de informação e comunicação da Gestão do Risco Operacional (GRO). Este compreende o registo, análise e reporte do risco operacional, assim como, garantir que todos os intervenientes tenham acesso oportuno e atualizado à informação relevante e possuam uma visão apropriada e objetiva das fontes de exposição ao risco.

O registo correto, sistemático, completo e transversal dos incidentes apresenta vantagens para o Banco, visto que permite:

- Identificar, monitorizar, avaliar, quantificar e analisar os riscos de forma uniforme;
- Aferir e melhorar as estimativas da probabilidade e impacto dos riscos;
- Atuar preventivamente sobre os incidentes ocorridos que podem causar impacto negativo na prossecução dos objetivos do Banco;
- Produzir dados estatísticos sobre os incidentes;
- Fornecer aos coordenadores das UE informação sobre os incidentes ocorridos.
- Obter indicadores chave de risco com base nos incidentes registados;

- Fornecer aos vários níveis de gestão, informação sobre os incidentes ocorridos.

Estes fatores alinhados à necessidade de se estabelecerem regras e princípios de funcionamento comuns a todo o Banco, justificam a necessidade da formalização de uma ferramenta de registo de incidentes mediante uma norma que consubstancia a sua utilização obrigatória por parte das Unidades de Estrutura (UE).

4.2.2. Caracterização de requisitos de Incidentes do DRI

Nesta secção, é descrito de forma sucinta e resumida, o levantamento e caracterização dos requisitos (mais detalhados nos anexos I e II).

Os incidentes devem ser registados por todos os colaboradores das UE que executam tarefas ou atividades, incluindo projetos que tenham, ou pudessem ter provocado um impacto negativo no Banco.

Devem ser registados os incidentes independentemente do seu impacto real, que se encontram incluídos na lista de incidentes de registo obrigatório, e ainda os incidentes considerados relevantes, seja pelo seu impacto, ou pela sua frequência, ou ainda pela sua utilidade para a gestão/tomada de decisão.

O registo de um incidente no DRI compreende duas (2) etapas:

- Caracterização do incidente: compreende a descrição e classificação do incidente, tendo em conta o evento, causas e impactos definidos;
- Análise do incidente: consiste no estudo dos incidentes por parte da UE onde ocorre, podendo ainda ser feita em conjunto com outras UE envolvidas.

Na segunda etapa, foram analisados os seguintes requisitos:

- Os incidentes devem ser registados por todos os colaboradores das UE que executam tarefas ou atividades, incluindo projetos que tenham, ou pudessem ter provocado um impacto negativo no Banco.
- Devem ser registados os incidentes independentemente do seu impacto real, que se encontram incluídos na lista de incidentes de registo obrigatório, e ainda os incidentes considerados relevantes, seja pelo seu impacto, ou pela sua frequência, ou ainda pela sua utilidade para a gestão/tomada de decisão.
- Encontram-se fora do âmbito de registo de incidentes, eventos do foro do Código de Conduta, que devem ser reportados diretamente ao Departamento de Recurso Humanos do Banco.

4.3. Processo de Gestão de Incidentes do DRI

Neste capítulo é analisado o processo de Gestão de Incidentes operacionalizado no Departamento de Gestão de Risco (DRI) do BNA, como parte integrante na Gestão de Risco.

Foram realizadas varias reuniões, até chegarmos a um processo definitivo que melhor se adeque as necessidades da instituição, nomeadamente da UE, na qual ficou definido o processo apresentado na seguinte figura.

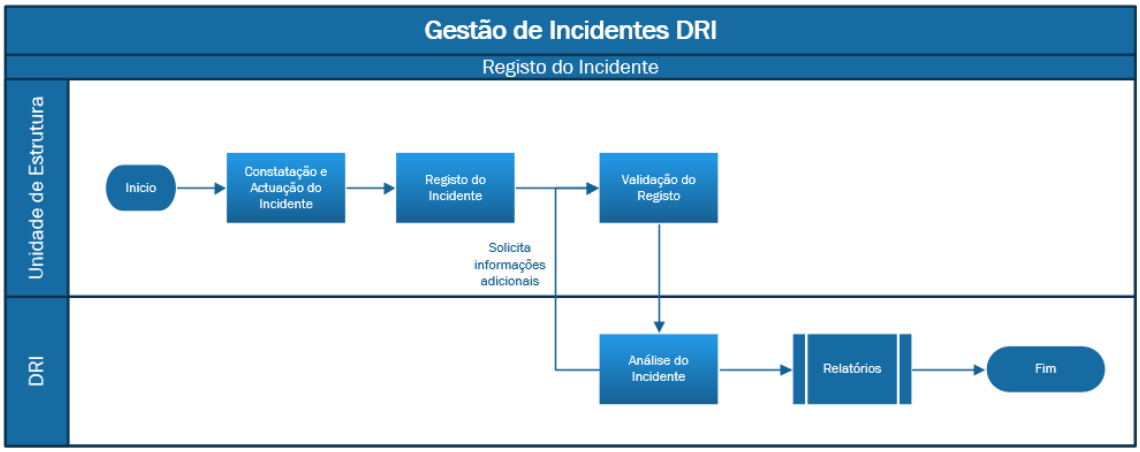


Figura 6 - Processo Gestão de Risco DRI

Fonte: DRI do BNA

O processo de gestão de incidentes DRI foi desenhado para funcionar da seguinte forma:

- Constatação e Atuação do incidente; procura-se responder (medida rápida para não deixar aumentar o acontecimento) perante o incidente.
- Registo do Incidente;
- Validação do Incidente;
    - Alerta de Novo Incidente;
    - Classificação dos eventos de risco.
    - Validação do registo dos incidentes, feita pelo Parceiro de Risco, para garantir que o evento foi registado corretamente.
    - Inclusão de documentos adicionais para análise do incidente (anexo).
- Análise do Incidente
    - Alerta de Novo Incidente;
    - Análise do incidente;
    - Avaliação de Correlações com outros incidentes;
- Relatórios

4.4. Processo de Gestão de Incidentes do DTI

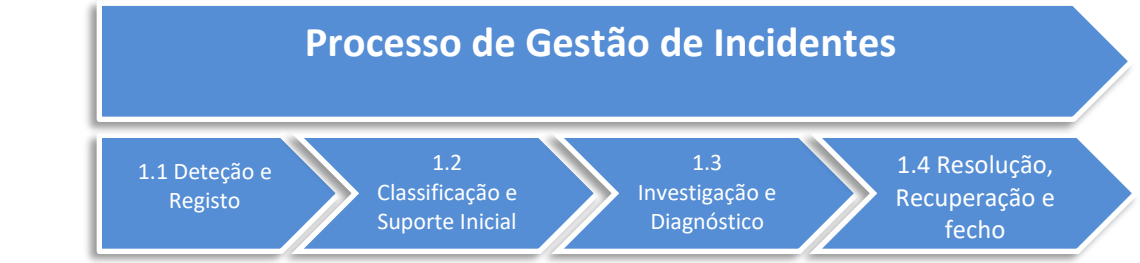
Nesta secção é feita uma síntese do processo de Gestão de Incidente (*Incident Management*) de TI implementado no DTI do BNA. O referido processo foi desenhado com base no *framework* ITIL.

O processo de Gestão de Incidente (*Incident Management*) tem como objetivo restaurar o serviço IT o mais rápido possível, minimizando o impacto negativo sobre os processos de negócios do BNA – quando se verifica algum tipo de falha ou perturbação ao normal funcionamento de um serviço IT.

Inclui todos os incidentes, que são comunicados diretamente pelos utilizadores dos serviços, seja através do portal de self-service ou através função de *Service Desk*, ou identificados através de interfaces (quando existentes) entre o sistema de gestão de incidentes e sistemas de deteção de evento (processo de *Event Management*). Para todos os incidentes é atribuído um código único e é ainda registada a data e hora em que ocorreram, para além de outra informação considerada relevante para meios de controlo, *reporting* e histórico (auditoria).

Este processo é dividido em 4 subprocessos:

- Deteção e Registo;
- Classificação e Suporte inicial;
- Investigação e diagnóstico;
- Resolução, recuperação e fecho.



	1.1 Deteção e Registo	1.2 Classificação e Suporte Inicial	1.3 Investigação e Diagnóstico	1.4 Resolução, Recuperação e fecho
Input	• Anormal funcionamento do serviço reportado	• Incidente registado ferramenta de *Service Desk*	• Suporte Inicial efetuado sem solução identificada	• Incidente investigado e diagnosticado com possível resolução identificada
Principais Atividades	• Registo de informação do utilizador, serviço afetado, sintomas, impacto e urgência.	• Pesquisa na BD de conhecimento de possíveis soluções; • Assignar incidente a grupos de 2ª linha; • Identificação de potenciais incidentes graves;	• Identificação da solução para o incidente • Assignar a fornecedores se necessário • Identificação de potenciais incidentes graves	• Implementar solução identificada • Confirmar resolução com o utilizador • Registo da solução encontrada no histórico do incidente
Intervenientes	• Cliente • *Service Desk*	• *Service Desk* • *Incident Manager*	• Equipas de 2ª Linha • *Service Desk* • *Incident Manager* • Fornecedores	• Equipas de 2ª Linha • *Service Desk* • *Incident Manager* • Cliente
Output	• Incidente registado com toda a informação necessária	• Incidente classificado priorizado • Incidente potencialmente resolvido • Assinação de incidentes complexos a técnicos de 2 linha	• Solução para o Incidente identificada • Potencial problema detetado	• Incidente resolvido e fechado • Reposição do serviço afetado a resolução aprovada pelo utilizador

Figura 7 - Processo Gestão de Incidentes

Fonte: BNA

Abaixo uma breve descrição de cada perfil (intervenientes), participantes no processo:

Perfil	Principais responsabilidades
Incident Management Process Owner	• Responsável por todo o processo, desde o seu início até a sua conclusão, e pela forma como o mesmo evolui e se desenvolve. O principal objetivo deste role é garantir que o processo é eficiente, eficaz e cumpre todos os objetivos definidos pela organização no âmbito do processo.
Incident Manager	• Responsável pela execução do processo, servindo de primeiro ponto de contacto com os restantes processos ITIL; • Gerir o trabalho e envolvimento de todos os intervenientes no processo, seja a equipa de *Service Desk* – 1ª linha –, equipas de 2ª linha ou fornecedores.
Service Desk	• Servir como PUC – Ponto único de contacto – para todos as interações dos diversos clientes e os serviços IT prestados pelo DTI. • Servir como primeira linha de suporte para a resolução de incidentes, identificando e implementando possíveis soluções, aumentando o grau de satisfação do cliente final.
Equipas de 2ª Linha	• Atuam como especialistas internos para a resolução de incidentes que não conseguem ser resolvidos num primeiro contacto pela equipa de *Service Desk*; • Criar os artigos para a base de dados de conhecimentos que sejam necessários para serem usados pela equipa de *Service Desk* e pelos próprios clientes na resolução de incidentes, minimizando o tempo de indisponibilidade dos serviços afetados.
Fornecedores (Equipa de 3ª Linha)	• Atuam como especialistas externos para a resolução de incidentes que não conseguem ser resolvidos internamente.

Tabela 2 - Perfis no Incident Management

Fonte: BNA

O referido projeto será aplicado apenas no subprocesso Deteção e Registo, do processo já implementado do BNA, Gestão de Incidentes.

4.4.1. Subprocesso Deteção e Registo

O principal objetivo deste subprocesso é providenciar uma metodologia *standard* para gerir a deteção, identificação e registo de todos os incidentes que provoquem ou possam vir a provocar falhas nos serviços TI. Tem como principais atividades detetar e identificar todos os incidentes que ocorrem na infraestrutura, documentar os contactos efetuados pelos clientes com o *Service Desk* e garantir que toda a informação necessária para efeitos de resolução, gestão e *reporting* é registada de forma consistente.

O registo deve conter toda a informação pertinente do utilizador (nome, meio de contacto, departamento associado), categoria do incidente, serviço afetado e sintomas verificados. Deve igualmente ser associada uma prioridade ao incidente, através da identificação da sua urgência e do seu impacto – este último por identificação do serviço afetado.

Este subprocesso tem como principal audiência os elementos da equipa de *Service Desk*, a equipa ou elemento responsável para gestão do processo de incidentes (*Incident Manager*). Deve igualmente ser conhecido pelas restantes equipas de 2ª linha, nomeadamente os elementos dos sectores de sistemas, redes e comunicações, gestão de base de dados e desenvolvimento aplicacional e ainda pelas equipas de controlo e gestão, nomeadamente os elementos dos sectores da Divisão de planeamento e gestão da qualidade e da segurança dos sistemas de informação.

Este subprocesso foi desenhado e implementado na solução CA Service Desk, na qual apresento abaixo:

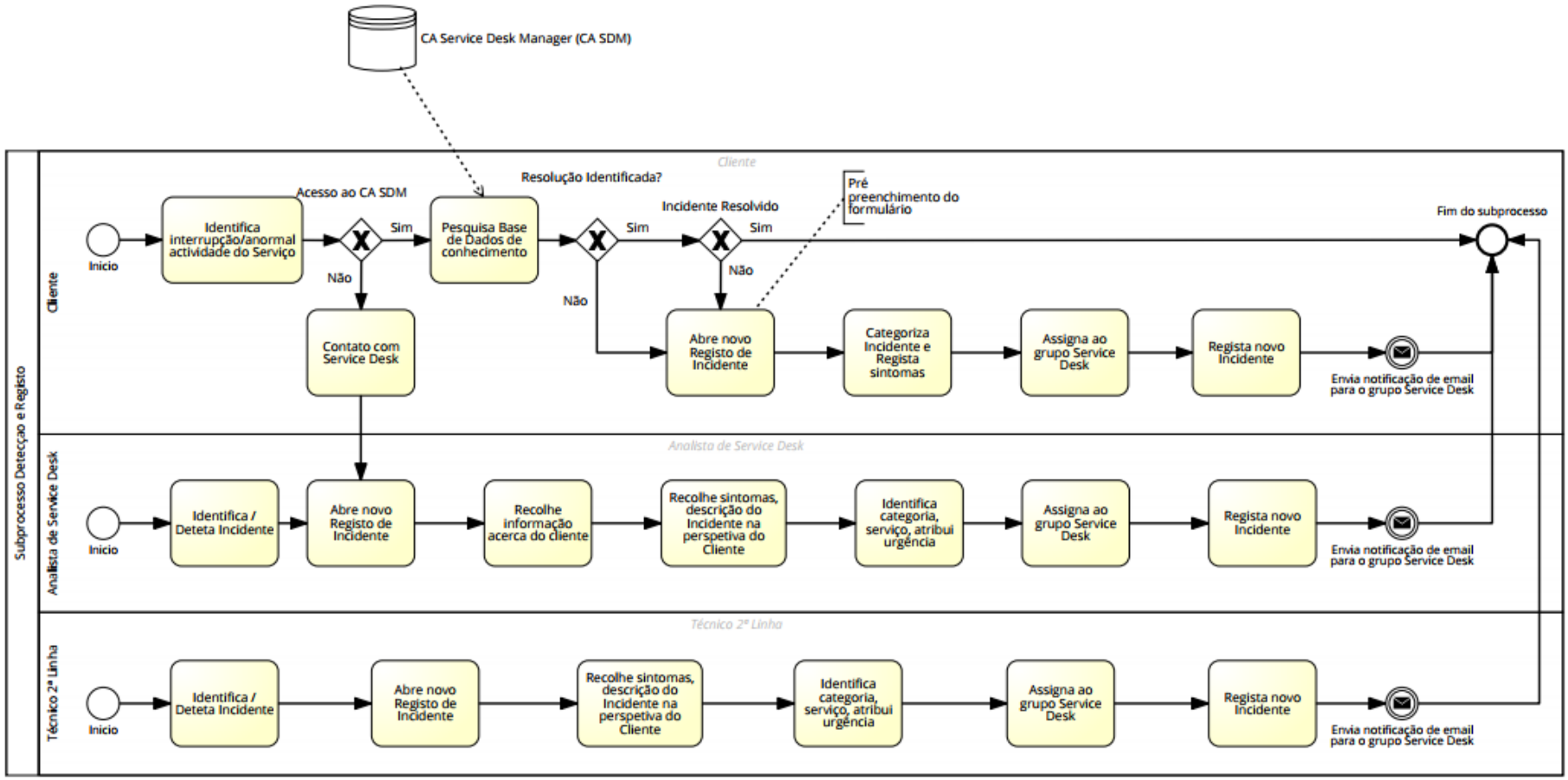


Figura 8 – Mapeamento do Subprocesso Deteção e Registo

Fonte: DTI do BNA

4.5. CA Service Desk Manager (CA SDM)

O ***CA SDM*** é um conjunto completo de funcionalidades de suporte e serviço, que vão desde pedidos de serviços, mudanças, incidentes, conhecimento e gestão de configurações para empresas de várias indústrias. O *CA SDM* é basicamente um aplicativo de mesa de serviço unificado que oferece todas as etapas e as operações da mesa de atendimento. Já uma plataforma poderosa, compacta e abrangente, o *CA SDM* também fornece aos usuários recursos de colaboração e social media integrados.

A aplicação tem como objetivo fazer a Gestão e registo de incidentes de T.I no Banco Nacional de Angola.

Uma das mais-valias da solução é a total flexibilidade em termos customização e parametrização para gestão de incidentes.

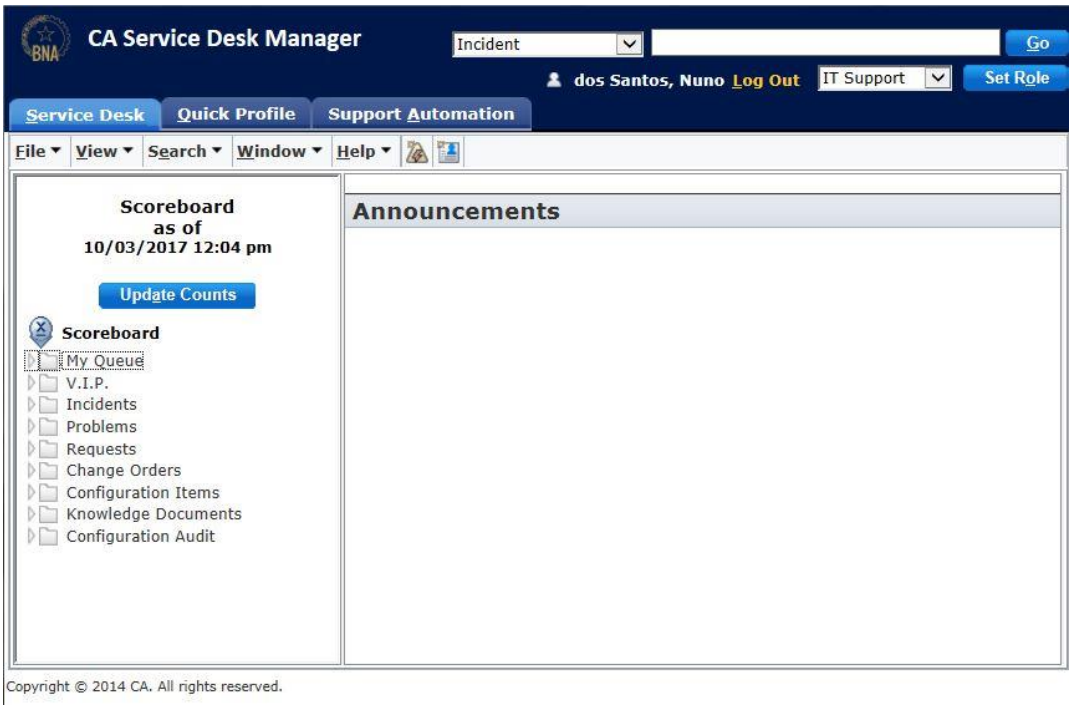


Figura 9 - Menu Inicial CA Sevice Desk

4.6. Implementação da Gestão de Risco no CA *Service Desk Manager*

Após análise exaustiva dos requisitos, chegou-se a conclusão que a ferramenta de registo de incidentes de risco (do DRI) poderá ser integrada na solução *CA SDM*, uma vez que a mesma responde aos requisitos e funcionalidades necessárias pelo cliente (DRI), no âmbito da GRO.

Diante disso, foi criada uma *framework* que resulta da integração do Processo Gestão de Incidentes de Risco do DRI (descrito no capitulo 3.2), com o subprocesso de Deteção e Registo do Processo de Gestão de Incidentes do DTI (descrito no capitulo 3.4.1).

O *Framework* criado, não só responde as necessidades de cliente (DRI) no âmbito da GRO, uma vez que todos incidentes que acontecem em toda as UE da instituição, têm agregado eventos de risco, bem como otimiza o sistema de gestão de Incidentes, fornecendo assim um ponto único de registo de incidentes transversal a instituição, mais completo e consolidado.

4.6.1. Análise e desenho do processo novo de registo de incidente

Tendo como base a literatura, abaixo apresento o mapeamento do subprocesso que passará a ser único para a Registo de Incidentes do BNA substituindo assim o subprocesso Deteção e Registo (descrito no capitulo 3.4.1), do Processo de Gestão de Incidentes de TI.

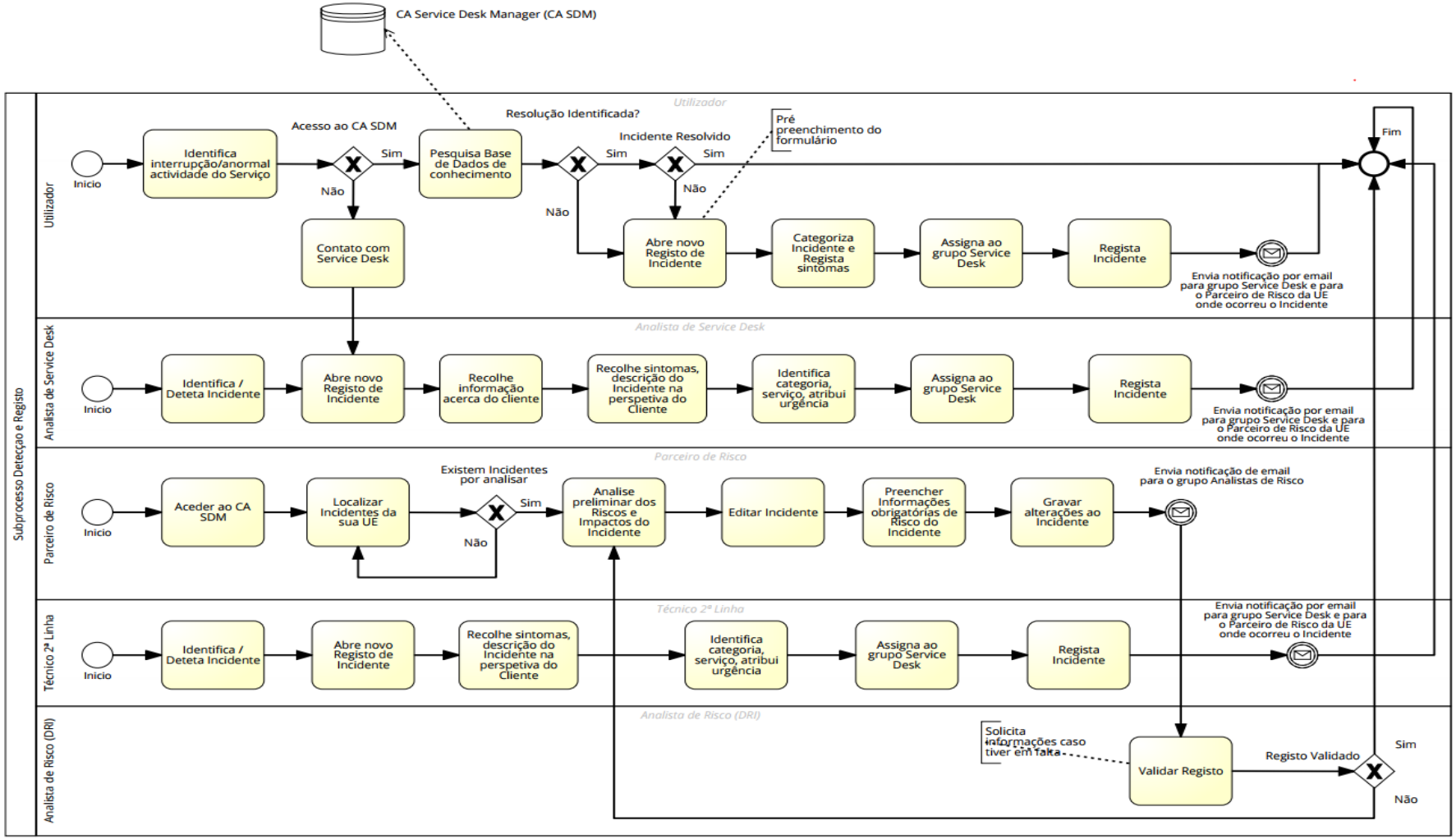


Figura 10 - Novo Processo de Registo de Incidente

Fonte: O autor

Com o referido processo conseguiu-se automatizar atividades que eram feitas manualmente pelos parceiros de risco, e os analistas de risco, conforme as normas e boas praticas referidas na literatura.

4.6.1. Implementação do processo novo de registo de incidente

Após o mapeamento deste processo, passamos a fase de desenvolvimento, no CA SDM. A empresa consultora procedeu a codificação em ambiente de desenvolvimento, sobre supervisão e apoio da equipa de projeto.

Foram criadas as tabelas, e consequentemente os campos relacionados com o Risco no formulário de registo de incidente, conforme ilustrado na imagens abaixo

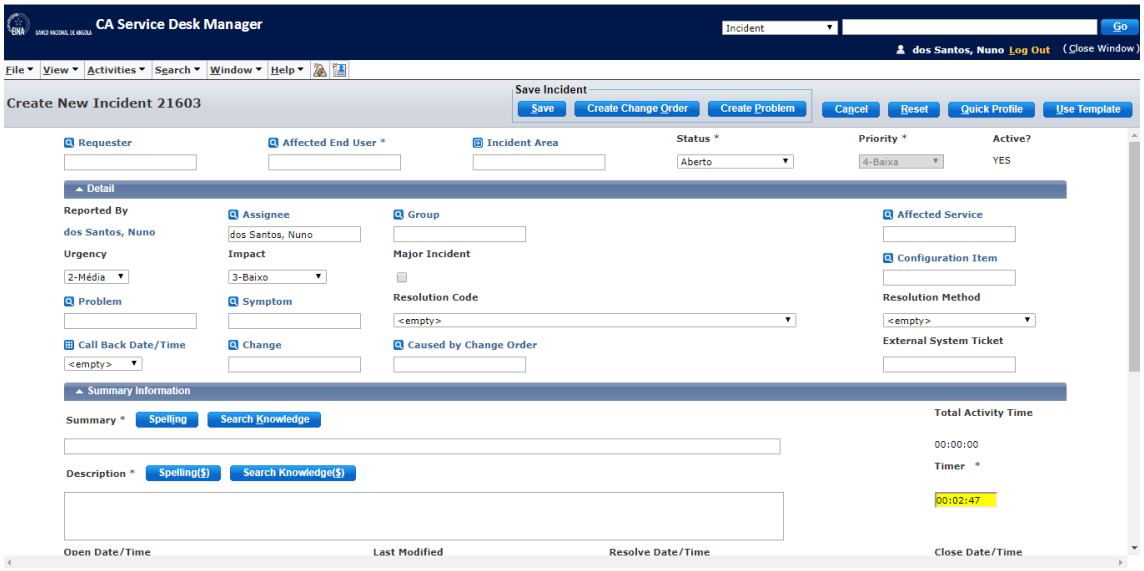


Figura 11 - Formulário Registo de Incidente

Esta parte do formulário não sofreu qualquer alteração, mantendo-se igual ao que se tem usado para registo dos incidentes (de TI). Foi apenas acrescentada uma aba para informações de risco, conforme imagem abaixo:

Figura 12 - Aba Classificação de Risco

Nesta aba do formulário, é onde é feita a classificação do risco (conforme tabelas no ANEXO III) no referido incidente. Para além da classificação do risco, foi criada a parte para tratamento do risco, conforme imagem abaixo:

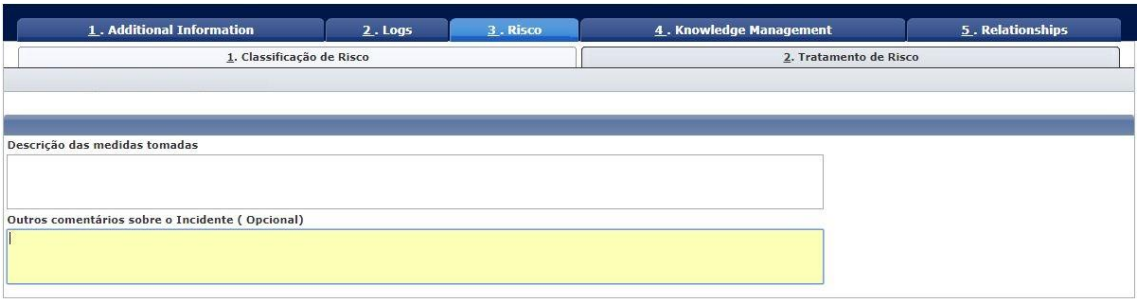


Figura 13 - Aba Tratamento do Risco

Os relatórios serão produzidos em *Power BI da Microsoft*, uma solução de Business *Intelligence* utilizada na instituição. A Parametrização no *Power BI* ficou pendente por parte do cliente, ficando ainda por definir os tipos de relatórios bem como as variáveis para extração das informações conforme necessidade. Porém, como ainda não foram parametrizados, será produzido provisoriamente na própria solução CA SDM.

4.7. Testes

Nesta fase foram realizados os testes, em ambiente de desenvolvimento, antes que seja passado para ambiente de produção. Foram realizados dois tipos de teste, o teste unitário, e o teste de Carga.

O teste unitário foi executado pela equipa de desenvolvimento, com o objetivo de examinar o comportamento do código diante de diversas condições, mais propriamente, apurar como o código se comporta diante de um parâmetro for ou não transposto, os resultados perante utilização de uma determinada condição verdadeira ou não, bem como as exceções.

Os testes de carga foram executados por duas equipas, a equipa de desenvolvimento e um administrador de sistemas (no caso eu). Com estes testes pretendia-se detetar bugs que não são detetados em ambientes normais de execução. Testes de carga são também capazes de detetar problemas relacionados com "*bufferoverflow*", "*memory leaks*" e má gestão de memória, além de determinar os limites dos recursos da infraestrutura do CA SDM, por exemplo, bases de dados, *hardware* e comunicação, etc. De forma a poder gerir e estimar a carga futura do sistema, uma vez que forma acrescentadas funcionalidades.

5. CONCLUSÕES, LIMITAÇÕES E RECOMENDAÇÕES FUTURAS

5.1. Conclusões

Em organizações complexas um incidente raramente ocorre de forma isolada, ultrapassa diversas medidas de proteção, resultando numa propagação e num incidente maior. Torna-se necessário criar diversas medidas, de modo a impedir a ocorrência de falhas e a propagação de determinados incidentes.

O registo de incidentes de risco uma é umas atividades importante da GRO, pois visa garantir que esses eventos atípicos sejam conhecidos por todos, reduzindo o impacto negativo e apurar os principais riscos a que o Banco está exposto. A *framework* criada, que resultou num sistema mais completo registo de incidentes, e classificação dos mesmos em termos de risco, vai servir como um instrumento de apoio ao processo de gestão de risco operacional, tendo em conta o histórico dos incidentes, com vista a apoiar na tomada de decisão. Sendo que atualmente o registo de incidentes de risco é feito através do preenchimento de um ficheiro Excel por cada UE, e depois compilada e analisada pelo DRI, tornando o processo pouco eficiente e desadequado, a ferramenta vai permitir os seguintes com que se alcance os seguintes benefícios:

- **Base de Dados de Incidentes**: construir uma base de dados de incidentes centralizada, completa, coerente, transversal ao Banco e de fácil manuseamento com informações de riscos sujeitos a cada incidente.

- **Redução do impacto negativo nas atividades do BNA**: permitir maior rapidez na resolução do incidente, reduzindo desta forma o impacto no negócio;
- **Elaboração de Indicadores Chave de Risco**: auxiliar na definição de KRIs (*Key Risk Indicator*), com base no registo dos incidentes ocorridos;
- **Apoio na tomada de decisão**: fornecer aos vários níveis de gestão, informação sistematizada dos incidentes ocorridos de modo a apoiar na tomada de decisão;
- **Criar uma cultura de registo de incidentes**: incentivar a participação dos colaboradores no registo consciente e responsável dos incidentes como consequência natural de quem executa tarefas/atividades.

5.2. Limitações

Uma das principais limitações foi o processo burocrático na aprovação do projeto, bem como a adjudicação do mesmo a empresa fornecedora da solução ***CA Service Desk Manager***.

Outra das limitações foi a falta de informações relacionadas com processos de outras áreas da instituição, por parte da U.E responsável pela documentação e mapeamento dos mesmos.

5.3. Recomendações Futuras

Recomenda-se que conforme se for aumentado o tempo e experiencia, e consequentemente a cultura de classificar os riscos, haverá a necessidade e integrar

funções que automatizem a análise dos dados na base de dados de incidentes, com uma solução de *Business Intelligence*.

O processo criado, pode ser otimizado, na medida que forem detetadas situações que afetem a correta operacionalização da mesma.

6. REFERÊNCIAS BIBLIOGRÁFICAS

Basel Committee on Banking Supervision (2006) *International Convergence of Capital Measurement and Capital Standards*.

Basel Committee on Banking Supervision (2003) 'Sound Practices for the Management and Supervision of Operational Risk Introduction', (February).

Basel Committee on Banking Supervision (2011) 'Principles for the Sound Management of Operational Risk', *Bank for International Settlements*, (June 2011), pp. 1–27.

Basel Committee on Banking Supervision. (2014). Basel III leverage ratio framework and, (January 2014).

van den Brink, G. J. (2002) *Operational Risk: The new challenge for banks*. 1st edn. Palgrave Macmillan UK.

Cartlidge, A*., Hanna, A., Rudd, I, MacFarlane, J., Windebank, J* , & *Rance, S.* (2007) *An introductory overview of ITIL V3*, *The UK Chapter of the itSMF*. doi: 10.1080/13642818708208530.

Cruz, M. (2002). Modelagem, avaliação e proteção para Risco Operacional. Rio de Janeiro: Financial Consultoria.

Decreto-Lei n.º 104/2007 de 3 de Abril do Ministério das Finanças e da Administração Pública. Diário da República n.º 66/2007, Série I de 2007-04-03. 2007.

Duarte, Jr. (1999) A importância do gerenciamento de riscos corporativos. Resenha BM&F. São Paulo.

Fernandes, A. , & Abreu, V. (2014) *mplantando a Governança de TI: da Estratégia à Gestão de Processos e Serviços*. 4ª.

Goguen, J. (1996). Formality and Informality in Requirements Engineering. In: International Conference on Requirements Engineering (ICRE '96), Colorado Springs, EUA. Proceedings…. IEEE Computer Society.

ISO. (2009). ISO 31000: Risk Management - Principles and guidelines, provides principles, framework and a process for managing risk.

ISO. (2009a). ISO Guide 73:2009: Risk management - Vocabulary complements ISO 31000 by providing a collection of terms and definitions relating to the management of risk.

Jiménez, E. (2013). El capital regulatorio por OpR–Tese de Doctoramento. Espanha: PubliCan Edic.–Univ. de Cantabria, Cuadernos de Investigación UCEIF, No 2/2011.

Jorion, P. (2000) *Value at Risk: The New Benchmark for Managing Financial Risk*. 2nd edn. McGraw-Hill.

Jorion, P. (2006) *Value at Risk: The New Benchmark for Managing Financial Risk*. 3rd edn. McGraw-Hill.

King, J. L. (2001) *Operational Risk: Measurement and Modelling*. Wiley Finance.

Kruchten, P. (2000). The Rational Unified Process: An Introduction. EUA: Addison-Wesley.

Laudon, K. , & Laudon, J. P. (2013) *Organizations, Management, and the Networked Enterprise*, *Management Information Systems, Global Edition*.

Macfarlane, I. , & Rudd, C. (2005) *Gerenciamento de Serviços de TI*. New Millenium Editora e Serviços gráficos Ltda.

Martins, P. L., Melo, B.M., Lemos, Q. D., Sousa, M.S. , & Borge, R. O. (2012) 'Tecnologia e Sistemas de Informação e Suas Influências na Gestão e Contabilidade', *Gestão, inovação e tecnologia para a sustentabilidade*, p. 13.

Nelson, S. C. & Katzenstein, P. J. (2008) 'Uncertainty , Risk , and the Financial Crisis of 2008', (2011), pp. 1–54.

Nuseibeh, B. , & Easterbrook, S. (2000) 'Requirements Engineering: A Roadmap', in *Proceedings of the Conference on The Future of Software Engineering*. New York, NY, USA: ACM (ICSE '00), pp. 35–46. doi: 10.1145/336512.336523.

O'brien, J. A. (2004). Sistemas de informação: e as decisões gerenciais na era da Internet. 2. ed. São Paulo.

Pedrosa, I., & Costa, C. J. (2012). Computer assisted audit tools and techniques in real world: CAATT's applications and approaches in context. *International Journal of Computer Information Systems and Industrial Management Applications*, *4*, 161-168.

Pressman, R. (2010) *Software Engineering: A Practitioner's Approach*. 7th edn. New York, NY, USA: McGraw-Hill, Inc.

Pressman, R. S. (1995) *Software Engineering: A Practitioner's Approach*. McGraw-Hill.

Pressman, R. S. (2001) *Software Engineering: A Practitioner's Approach*. 5th edn. McGraw-Hill Higher Education.

Ribeiro, P. C.C. , & Vieira, L. S. (2001). Tecnologia da Informação e Competitividade na Indústria Siderúrgica Brasileira: um Estudo de Caso na CSN. Revista de Economia da Universidade de Santa Catarina.

Schutzer, E. , & Pereira, N. A. (1999). Sistemas de informação. In: Gestão Agroindustial. Grupo de Estudos e Pesquisas Agroindustriais – GEPAI. São Paulo: Atlas, 1999.

Siddiqi, J. , & Shekaran, M. C. (1996). Requirements Engineering: the emerging wisdom. IEEE Software, v. 13.

Silva, M., & Martins, J (2008). IT Governance, A Gestão da Informática. FCA

Sironi, A. , & Resti, A. (2007) *Risk Management and Shareholders' Value in Banking: From Risk Measurement Models to Capital Allocation Policies*. Edited by Wiley Finance.

Sommerville, I. (2007) *Software Engineering*. 8th edn. Addison-Wesley.

Spinola, M. , & Pessôa, M. (1998). Tecnologia da Informação: Gestão de Operações. 2a ed. Professores do Departamento de Engenharia da escola Politécnica da USP e da Fundação Carlos Alberto Vanzolini. São Paulo: Editora Edgard Blücher, cap.7

Tschoegl, A. (2005) 'The key to risk management: management', *Risk Management*.

Ventura, J. (1992), Impactos dos Sistemas de Informação e das Tecnologias da Informação nas Organizações - Um contributo para a sua inventariação e Avaliação, Dissertação de Mestrado.

Zanlorenci, E. (1999). Descrição E Qualificação De Requisitos: Um Modelo Aplicável À Análise E Validação Da Informação. Dissertação de Mestrado, Curso de Pós-Graduação em Informática Aplicada. PUCPR.

Zave, P. (1997). Classification of Research Efforts in Requirements Engineering. ACM Computing Surveys. v. 29, n. 4.

ANEXO I

Campos do formulário

1. Referência (ID) do incidente;

   Campo de preenchimento automático.

2. Classificação do Incidente (Lista da Taxonomia dos Eventos)

   Campo em *drop down list* de preenchimento obrigatório.

3. Descrição do Incidente;

   Campo de texto, de preenchimento obrigatório.

4. Processo onde ocorreu (lista de processos);

   Campo em *drop down list*, de obrigatoriedade de preenchimento ainda por definir.

5. Tipo de incidente (lista Operacional/Conformidade);

   Campo em *drop down list* de preenchimento obrigatório.

6. Duração do incidente

   - Campo com Data/Hora de início (preenchimento obrigatório);
   - Campo com Data/Hora de fim (preenchimento opcional);

7. Incidente já ocorreu alguma vez

   Campo "Sim" ou "Não". Obrigatoriedade de preenchimento ainda por definir.

8. Causas do incidente (lista da Taxonomia das Causas)

   Campo em *drop down list* de preenchimento obrigatório.

9. Impacto do incidente (lista da Taxonomia dos impactos);

   Campo em *drop down list* de preenchimento obrigatório.

10. Nível de impacto (lista da Taxonomia das Causas);

    Campo em *drop down list* de preenchimento obrigatório.

11. O incidente afetou a continuidade do negócio/atividade

    Campo “Sim” ou “Não”. Obrigatoriedade de preenchimento ainda por definir.

12. Descrição das medidas tomadas

    Campo de texto, preenchimento obrigatório

13. O incidente é transversal a outras UE

    Campo “Sim” ou “Não”. Caso for “Sim”, deverá identificar a UE. Preenchimento obrigatório.

14. Plano de ação

    Campo “Sim” ou “Não”. Obrigatoriedade de preenchimento ainda por definir.

15. *Status* do incidente

    Lista “Resolvido”, “Não resolvido” e “Em curso”. Preenchimento obrigatório.

16. Outros comentários

    Campo de texto, de preenchimento opcional.

ANEXO II

Requisitos

[R1] Integração com o CA *Service Desk Manager*

O sistema de registo de incidentes de Risco, deverá ser integrado na solução de *Service Desk Manager*, que é a solução de registo e gestão de incidentes de TI.

[R2] Autenticação

A semelhança do CA *Service Desk Manager*, a autenticação dos utilizadores no sistema de registo de incidentes de Risco será feita por *Active Directory*, por LDAP.

[R3] Acesso ao sistema

O acesso ao sistema é feito por *Single Sign On* (SSO), uma vez que o acesso será feito ao CA *Service Desk Manager*. O acesso deve ser para todos utilizadores de todas EU.

[R4] Perfis

Os perfis definidos são os seguintes:

- Administrador

Gerir toda a informação de parametrização do sistema, perfis e autorizações de acesso ao sistema.

- Utilizador

Perfil que permite registar incidentes de risco. Modificar e visualizar os incidentes que foram registados por si.

- Parceiro de Risco

Perfil que permite registar incidentes de risco. Modificar e consultar os incidentes que foram registados por si. Perfil que permite registar classificar os incidentes respetivos a sua UE, editar e classificar os incidentes que foram registados por utilizadores da sua UE.

- Analista de Risco

Consultar todos os incidentes registados, validar o preenchimento de campos obrigatórios a serem preenchidos pelo parceiro de Risco, e notificar no caso da falta de alguma informação. Perfil com acesso a gerar relatórios.

- Auditor interno

Consultar toda informação presente na base de dados de incidentes.

[R5] Interface do Painel principal

O sistema de registo de incidentes deverá ter uma interface de fácil manuseamento, que permita uma visão clara e sequencial das suas funcionalidades.

[R5] Parametrizações

O sistema de registo de incidentes deverá permitir algumas funcionalidades de parametrização:

- Gestão de perfis /acessos;
- Delegações de perfis (funcionalidade prevista para ausência do parceiro de risco das EU)

ANEXO III

Lista da Taxonomia dos Eventos

Categorias de Eventos de Risco- Nível 1 (Basileia)	Categorias de Eventos de Risco - Nível 2
1. Fraude interna	1(a) – Atividades, transações e posições não autorizadas
	1(b) – Roubo e fraude internos
2. Fraude Externa	2(a) – Sistemas de segurança
	2(b) – Roubo e fraude externos
3. Gestão de Pessoas e Segurança do Trabalho	3(a) – Relações com funcionários, leis e regulamentos
	3(b) – Leis e regulamentos do ambiente de de saúde e segurança do trabalho
	3(c) – Leis e regulamentos sobre diversidade e discriminação
4. Clientes, Produtos e Negócio	4(a) – Integridade e *disclosure* de informações
	4(b) – Desenvolvimento de produtos e serviços
	4(c) – Práticas de negócios e de mercado
	4(d) – Atividades terceirizadas
	4(e) – Seleção de cliente e exposição a este cliente
5. Interrupção do Negócio e Falhas de Sistemas	5(a) – Sistemas operacionais
	5(b) – Desenvolvimento de sistemas
	5(c) – *Change management*
	5(d) – Serviços
6. Danos aos Ativos Físicos	6(a) – Desastres e outros eventos físicos
7. Gestão da Execução, Entrega e Processos	7(a) – Gerenciamento de contas de clientes
	7(b) – Segurança de dados
	7(c) – Criação / manutenção de documentação de clientes e informações de conta
	7(d) – Contrapartes
	7(e) – Execução e captura de transações
	7(f) – Execução operacional e manutenção
	7(g) – Manutenção da Contabilidade
	7(h) – Monitoramento e reporte
	7(i) – Fornecedores e terceirização de produtos / serviços

Lista de Níveis de Impacto

Escalas / Níveis	Critérios de Impacto				
	Objetivo de Negocio	Reputação e Imagem		Financeiro	*Compliance* / Legal
		Credibilidade	Missão	Estimativas	
1	Sem impacto no cumprimento da missão do BNA.	A credibilidade é afetada de forma insignificante (menos de uma semana);	Sem incumprimento de compromissos legais, contractuais e de *Compliance*.	Por definir	Sem incumprimento de compromissos legais, contractuais e de *Compliance.*
2	Sem impacto no cumprimento da missão do BNA.	A credibilidade é afetada a muito curto prazo (1 semana a 3 meses)	Imputação de perdas financeiras por parte do SFA (1 Banco Comercial)	Por definir	Imputação de perdas financeiras por parte do SFA (1 Banco Comercial)
3	Sem impacto no cumprimento da missão do BNA.	A credibilidade é afetada a curto prazo (3 meses a 1 ano)	Imputação de perdas financeiras por parte do SFA (até 5 Bancos Comerciais); Pedido de esclarecimentos do Estado ao BNA	Por definir	Imputação de perdas financeiras por parte do SFA (até 5 Bancos Comerciais); Pedido de esclarecimentos do Estado ao BNA; Imputação de perdas financeiras por parte do SFA (até 5 Bancos Comerciais); Pedido de esclarecimentos do Estado ao BNA.
4	Forte possibilidade de incumprimento da missão do BNA: - Definir e executar e controlar as políticas monetárias, crédito e cambial; - Gerir o Sistema de Pagamentos Angolano; - Atuar como Banco único do Estado	A credibilidade é afetada a médio prazo (1 a 3 anos)	Imputação de perdas financeiras por parte do SFA (até 10 Bancos Comerciais); Multas e dificuldade de acesso aos mercados internacionais através dos Bancos correspondentes e SGAs; Investigação do Estado ao BNA; Notificações, observações ou recomendações por parte do FMI, Banco Mundial, Reserva Federal Americana, GAFI ou BCE.	Por definir	Imputação de perdas financeiras por parte do SFA (até 10 Bancos Comerciais); Multas e dificuldade de acesso aos mercados internacionais através dos Bancos Correspondentes e SGAs; Investigação do Estado ao BNA; Notificações, observações ou recomendações por parte do FMI, Banco Mundial, Reserva Federal Americana, GAFI ou BCE.

Escalas / Níveis	Critérios de Impacto				
	Objetivo de Negocio	Reputação e Imagem		Financeiro	*Compliance* / Legal
		Credibilidade	Missão	Estimativas	
5	Incumprimento da missão do BNA.	A credibilidade é afetada de forma duradoura (> 3 anos)	Imputação de perdas financeiras pelo SFA (todos os Bancos Comerciais); Impossibilidade de acesso a mercados internacionais devido a descontinuidade de contas do BNA nos Bancos Correspondentes e SGAs; Prestação de esclarecimentos na Assembleia Nacional; Aplicação de sanções por parte do FMI, Banco Mundial, Reserva Federal Americana, GAFi ou BCE.	Por definir	Imputação de perdas financeiras pelo SFA (todos os Bancos Comerciais); Impossibilidade de acesso a mercados internacionais devido a descontinuidade de contas do BNA nos Bancos Correspondentes e SGAs; Prestação de esclarecimentos na Assembleia Nacional; Aplicação de sanções por parte do FMI, Banco Mundial, Reserva Federal Americana, GAFi ou BCE.

Taxonomia das Causas

Objetivo de Negocio		
Categorias	Subcategorias	Exemplos
Governação e Processos de Negócio	Estratégias e processos de decisão	Políticas e processos de governação interna ou de tomada de decisão inadequados, incluindo delimitações de competências e responsabilidades interdepartamentais.
	Organização e definição de competências, funções e responsabilidades	Segregação de funções inexistente ou deficiente, ou possibilidade de que alguém isoladamente possa subverter um processo ou operação crítica;
		Deficientes sistemas ou processos de conferência, autorização e monitorização das operações;
	Estabelecimento de Planos, Objetivos e Metas.	Política de planeamento e controlo inadequada;
		Políticas, regras e orientações inadequadas de planeamento, de orçamentação e de reporte financeiro e de gestão;
	Processos Operacionais	Políticas e procedimentos inadequados para prevenir, detetar ou corrigir erros operacionais gerais; Processos inadequados de gestão de registos e documentos de suporte às operações;
	Gestão de Projetos	*Standards* inadequados de desenvolvimento de projetos;
		Deficiente alinhamento dos projetos com os objetivos estratégicos;
	Infraestrutura e Segurança Física	Políticas, procedimentos ou práticas deficientes de utilização das infraestruturas, equipamentos e outros meios físicos e técnicos associados;
		Sistemas de segurança física deficientes ou inadequados.
	Informação e Comunicação	Processos inadequados de obtenção e comunicação da informação relevante de origem interna e externa, incluindo fontes, canais e ferramentas de recolha e comunicação;
		Processos de relacionamento com o público deficiente ou inadequado.
	Conformidade com a Legislação, regulamentos e contratos	Incumprimentos da legislação, regulamentos e regras aplicáveis;
		Políticas, regulamentos, procedimentos e práticas de aquisição e contratação e gestão de contratos inadequados.
Pessoas	Meios Humanos (Qualidade e Quantidade, Gestão e Motivação).	Incumprimento das políticas e requisitos de desempenho profissional e de cumprimento dos deveres profissionais;
		Competências e habilidades necessárias inadequadas;
		Falta de programas de formação e desenvolvimento adequados;

Objetivo de Negocio		
Categorias	Subcategorias	Exemplos
	Princípios éticos e de conduta.	Políticas e procedimentos inadequados de prevenção, deteção e tratamento de situações de conflito de interesses.
	Política de Trabalho e Emprego.	Políticas, regulamentos e práticas de Emprego, Saúde e Segurança no trabalho inadequadas
Sistemas	Gestão de SI/TI	Governação inadequada de Sistemas de Informação;
		Processos de gestão do risco e controlo IT/IS inadequados;
		Políticas, procedimentos, controlos e medidas de proteção da informação considerada como ativo crítico do Banco inadequadas;
		Aplicações deficientes ou não ajustadas aos requisitos de negócio.
	Gestão de Infraestruturas de TI e Comunicações	Governação inadequada das infraestruturas de redes e comunicações;
		Infraestruturas de redes e comunicações deficientes ou inadequadas;
	Segurança da Informação (disponibilidade, confidencialidade, integridade e Controlabilidade)	Procedimentos de gestão e controlo de acessos inadequados;
		Políticas e procedimentos inadequados de salvaguarda da disponibilidade de dados e sistemas, incluindo soluções de *backup* e recuperação;
		Falhas de sistemas ou estruturas de comunicação.
Eventos Externos	Falhas de Entidades ou Sistemas Externos	Políticas e procedimentos de segurança inadequados para responder a ataques externos, incluindo terrorismo, vandalismo sabotagem, invasão, cerco, chantagem, etc.;
		Deficiente acompanhamento e avaliação dos riscos para o Banco inerentes às alterações e tendências políticas, sociais, económicas e tecnológicas.
	Acidentes e Catástrofes naturais	Deficiências do PCN de forma a responder a desastres e catástrofes naturais, incluindo situações de pandemia.

Taxonomia dos Impactos

TAXONOMIA DOS IMPACTOS DOS RISCOS		
Categoria	Definição	Exemplos
Objetivos de Negócio	Falha ou deficiências nos objetivos e/ o nas funções, tarefas, processos, operações ou projetos do Banco decorrentes da legislação, regulamentos, contratos, outras normas obrigatórias ou decorrentes dos objetivos estratégicos e operacionais estabelecidos.	Falha ou impossibilidade de assegurar a missão estatutária ou decorrente de normas obrigatórias.
		Falha em alcançar os objetivos estratégicos.
Reputação e Imagem	Deterioração da reputação, credibilidade ou imagem pública do Banco em relação aos seus "*stakeholders*" externos (Estado, SEBC, Público, Sector Financeiro, etc.).	A reputação é afetada de forma duradoura por divulgação de informação não credível.
		Falta/quebra de confiança pública junto dos *stakeholders* externos.
Financeiro	• Perdas financeiras diretas e indiretas deduzidas de eventuais indemnizações e garantias recebidas; • Penalidades legais; • Custos de recuperação e correção de sistemas e processos; • Custos de oportunidade (incluindo lucros perdidos).	Perdas decorrentes de multas ou infrações cometidas pelo Banco.
		Incumprimento decorrentes de compromissos financeiros contratualmente estabelecidos.
		Movimentação desfavorável nos preços de mercado dos instrumentos da carteira de negociação, ameaçando os recursos e cash *flows* futuros do Banco.
***Compliance*/Legal**		• Incumprimento de compromissos legais, contractuais e de *Compliance*; • Imputação de perdas financeiras por parte do SFA (1 Banco Comercial); • Multas e dificuldade de acesso aos mercados internacionais através dos Bancos Correspondentes e SGAs;

TAXONOMIA DOS IMPACTOS DOS RISCOS		
Categoria	Definição	Exemplos
		• Notificações, observações ou recomendações por parte do FMI, Banco Mundial, Reserva Federal Americana, GAFI ou BCE; • Impossibilidade de acesso a mercados internacionais devido a descontinuidade de contas do BNA nos Bancos Correspondentes e SGAs; • Aplicação de sanções por parte do FMI, Banco Mundial, Reserva Federal Americana, GAFi ou BCE.